



Report of the Vermont State Auditor

February 16, 2007

FISCAL YEAR 2006

Report on Internal Control Over Financial Reporting and on Compliance with Laws and Regulations

Thomas M. Salmon, CPA
Vermont State Auditor
Rpt. No. 07-07

Mission Statement

The mission of the Auditor's Office is to be a catalyst for good government by promoting reliable and accurate financial reporting as well as promoting economy, efficiency, and effectiveness in state government.

This report is a work of the Office of the State Auditor, State of Vermont, and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from the State of Vermont or the Office of the State Auditor. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately. Please contact the Office of the State Auditor if you have questions about reproducing this report.



**STATE OF VERMONT
OFFICE OF THE STATE AUDITOR**

**Report on Internal Control Over Financial Reporting and On Compliance
and Other Matters Based on An Audit of Financial Statements
Performed in Accordance With Government Auditing Standards**

Speaker of the House of Representatives Gaye Symington
President Pro Tempore of the Senate Peter D. Shumlin
Governor James Douglas
Secretary of the Agency of Administration, Michael K. Smith
Commissioner of the Department of Finance & Management, James Reardon
Commissioner of the Department of Information and Innovation, Thomas Murray

Dear Colleagues:

We have audited the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Vermont, as of and for the year ended June 30, 2006, which collectively comprise the State of Vermont's basic financial statements, and have issued our report thereon dated December 31, 2006. Our report was modified to include a reference to other auditors. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Other auditors audited the financial statements of the component units and certain business-type activities, as described in our report on the State of Vermont's basic financial statements. This report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters that are reported on separately by those auditors.

Internal Control Over Financial Reporting

In planning and performing the audit, we considered the State of Vermont's internal control over financial reporting in order to determine auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide an opinion on internal control over financial reporting. However, we noted certain matters involving internal control over financial reporting and its operation that we consider to be reportable conditions. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control over financial reporting that, in our judgment, could adversely affect the State of Vermont's ability to initiate, record, process and report financial data consistent with

the assertions of management in the financial statements. Reportable conditions are described in the accompanying schedule of findings and responses, appendix I, as items 2006-1, 2006-2 and 2006-3, and includes recommendations for improvement. Appendix II contains a reprint of management's responses. A summary of the findings follows.

Compilation of the Comprehensive Annual Financial Report #2006 - 1. Weaknesses were noted in the Department of Finance & Management's internal controls related to compiling the comprehensive annual financial report ("CAFR"). These weaknesses include (1) inadequate segregation of duties and management review of key data and (2) limited monitoring of decentralized accounting processes occurring at multiple agencies and departments. We noted significant errors, prior to audit adjustments, which resulted from these weaknesses.

Technical Accounting and Financial Management Expertise #2006 - 2. The financial statement compilation process, heavily reliant upon decentralized accounting processes at agencies and departments, was negatively impacted by personnel with limited accounting and financial reporting expertise performing key accounting and financial reporting functions. We found significant errors, prior to audit adjustments, which resulted from key financial positions being staffed with personnel lacking adequate accounting and financial reporting knowledge, skills and abilities.

Information Technology Controls #2006 - 3. Weaknesses were found in a variety of general control areas, including overall security planning, access to data and programs, program changes, and computer operations. One factor that contributed to these weaknesses is that existing statewide security policies are outdated and are not comprehensive.

A material weakness is a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Our consideration of the internal control over financial reporting would not necessarily disclose all matters in internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses. The reportable conditions described above are not considered to be material weaknesses.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the State of Vermont's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

We noted certain matters that we will report to management of the State of Vermont in a separate letter.

This report is intended solely for the information and use of the Speaker of the House of Representatives, the President Pro-Tempore of the Senate, the Governor, the Secretary of the Agency of Administration, the Commissioner of the Department of Finance & Management and the head of relevant state agencies, departments or institutions. However, this report is a matter of public record and its distribution is not limited.

Thomas M. Salmon CPA

Thomas M. Salmon, CPA
State Auditor
December 31, 2006¹

¹December 31, 2006 represents the date that fieldwork was substantially complete under Randolph D. Brock, the prior State Auditor. This report was issued subsequent to the date Thomas M. Salmon was inaugurated as the State Auditor.

Appendix I

Schedule of Findings and Responses

This appendix identifies the reportable conditions related to the financial statements that are required to be reported in accordance with *Government Auditing Standards*.

Control Finding #2006-1 Compilation of the Comprehensive Annual Financial Report

As we have reported in previous years, and noted again during our fiscal year 2006 audit, there are weaknesses in the Department of Finance & Management's internal controls related to compiling the comprehensive annual financial report ("CAFR"). These weaknesses include (1) inadequate segregation of duties and management review of key data and (2) limited monitoring of decentralized accounting processes occurring at multiple agencies and departments.

Segregation of Duties and Management Review

Adequate segregation of duties is the practice of dividing the steps in a critical function among different individuals in order to reduce the risk of error, thus preventing an individual from having full control of a transaction or event. Appropriate reviews by management of key decisions and data are vital controls to ensure that only authorized transactions occur and to reduce the risk of error. Lack of segregation of duties and management review for critical processes leaves the CAFR vulnerable to errors and could result in incomplete and inaccurate summarization of data within the financial statements.

During our fiscal year 2006 audit, we found that the Finance & Management department's management personnel performed certain detailed accounting functions themselves, that were not reviewed by others. This did not allow for adequate segregation of duties and precluded management review of data. We noted three errors, prior to audit adjustments, which resulted from inadequate segregation of duties and lack of management review.

- (1) The Bond Refundings footnote, as originally drafted, omitted the required disclosure of \$61 million of fiscal year 2004 defeased bonds¹ outstanding

¹Defeased bonds result from the issuance of new debt to refinance existing ("old") debt. In the case of defeased bonds, the proceeds of the refunding debt are placed into an escrow account pending the call date or maturity of the old debt. For accounting purposes, the debt is treated as if it had been redeemed.

Appendix I

Schedule of Findings and Responses

at June 30, 2006. In addition, the footnote included \$28.1 million of fiscal year 1998 defeased bonds which had already been repaid.

- (2) The General Obligation Bonds Payable footnote, as originally drafted, overstated interest payable. \$23.4 million of capital appreciation interest was stated separately and was also reported in future interest payments, resulting in an overstated obligation for interest payable.
- (3) The allocation of the Medicaid Payable to the Global Commitments Fund was overstated by \$15.8 million, prior to audit adjustment, due to an error in the calculation.

To reduce risk of error, information should be compiled and transactions should be executed by certain individuals and then reviewed and approved by others.

Management performance of staff functions indicates inadequate staff resources or lack of depth of staff experience and may cause undue workload for management. We found that management had excessive workloads and an extraordinary amount of effort and dedication was required to compile the CAFR. In addition, too few Finance & Management personnel have the specialized financial reporting expertise necessary to ensure accurate and reliable financial reporting. There is heavy reliance on a single individual to perform key functions. If this individual were unavailable, Finance & Management's financial reporting process would be negatively affected.

Recommendations

We recommend that the Commissioner of the Department of Finance & Management implement a program of technical accounting and functional position training for Finance & Management staff accountants.

We recommend that the Commissioner of the Department of Finance & Management recruit a managerial level individual with significant technical accounting experience and broad depth of understanding of government operations.

Oversight of Decentralized Accounting Processes

Timely and reliable financial reporting in an environment of decentralized accounting processes is largely dependent upon appropriate oversight and guidance provided to individuals performing the accounting and financial management function at the decentralized locations.

Appendix I

Schedule of Findings and Responses

During our fiscal year 2006 audit, we found significant errors in the governmental fund financial statements. Prior to audit adjustments, expenditures were understated by approximately \$7.8 million and revenue was understated by \$2.9 million due to errors at the agency and department levels. (See the reportable condition 2006 – 2 concerning lack of accounting and financial expertise at agencies and departments for detail of these errors.) Review of fluctuation analyses for year-to-year changes in account balances is the key oversight control relied upon by Finance & Management to detect errors in financial results reported by agencies and departments. However, these analyses failed to detect significant errors in period end cut-off for expenditures and in the incorrect classification of certain transactions as revenue. Accounting and reporting guidance provided to agencies and departments by Finance & Management primarily consisted of Year End Closing Instructions and did not serve as a comprehensive reference source for accounting and financial management personnel.

Recommendations

To improve the oversight provided by the Department of Finance & Management, we recommend the following to the Commissioner of the Department of Finance & Management:

- (1) Production of an accounting policies and procedures manual to be made available to agency personnel as a reference guide for accounting transactions and financial reporting.
- (2) Review of the compilation process to determine whether additional oversight controls over the agencies' financial accounting could be designed to operate at a level sufficient to identify the types of errors noted during the fiscal 2006 audit.

Management's Response and Planned Corrective Actions

The Commissioner of the Department of Finance & Management responded to a draft of this report (reprinted in appendix II). Although the Commissioner did not explicitly address each of the specific recommendations that we made, he provided information on actions that his office has taken, and plans to take, to address the two major issues outlined in this control finding, as follows:

- *Segregation of Duties and Management Review.* According to the Commissioner, the Department of Finance & Management, (1) has a knowledge transfer training program in place in which the ultimate goal is to have the staff develop all statements and footnotes so that the Director

Appendix I

Schedule of Findings and Responses

of State-wide Reporting can be limited to a review role; (2) has begun recruiting for a senior-level staff person to assume the bulk of the CAFR compilation; and (3) plans to investigate attendance by selected staff members to training seminars and certification programs sponsored by the Government Finance Officers Association.

- *Oversight of Decentralized Accounting Process.* The Commissioner stated that staffing levels do not allow the Department of Finance & Management to directly monitor the quality and accuracy of thousands of transactions entered by agency and departmental staff, but agreed that improvements could be made. He stated that the Department's Division of Internal Controls has begun operational reviews of departments and specific processes. These reviews include corrective action reports and are supplemented by the issuance of best practices to the State's financial community. The Commissioner noted that better training and hiring of better qualified staff at the agencies/departments is critical to the quality of the accounting transactions.

The actions that the Department of Finance & Management has taken, and plans to take, are positive steps in addressing our concerns related to the compilation of the CAFR. However, we continue to believe that additional actions are needed, as outlined in our recommendations.

First, while the knowledge transfer training program described is a very constructive step, the nature of such a program is typically to convey information on how things were done in the past and is not usually geared towards dealing with future challenges, such as changes in the accounting profession and new State programs, such as the Global Commitment Program, that require a thorough understanding and grounding in accounting theory to address how they should be reported. Accordingly, we continue to believe that a more formal program of technical accounting and functional position training would be beneficial.

Second, the Commissioner did not address our recommendation to produce an accounting policy and procedures manual to be made available to agency personnel. We believe that the production of such a manual would help mitigate the issue of the staffing levels at the Department of Finance & Management and the need for better training and hiring at the agency/department level that was noted by the Commissioner.

Appendix I

Schedule of Findings and Responses

Control Finding #2006-2 Technical Accounting and Financial Management Expertise

The commitment to hiring and developing competent and knowledgeable personnel is a critical component of the control environment. During our fiscal year 2006 audit, we found that the financial statement compilation process, heavily reliant upon decentralized accounting processes at agencies and departments, was negatively impacted by personnel with limited accounting and financial reporting expertise performing key accounting and financial reporting processes.

We found significant errors in the governmental fund financial statements that resulted from key financial positions being staffed with personnel lacking adequate accounting and financial reporting knowledge, skills and abilities. Prior to audit adjustments, expenditures were understated by approximately \$7.8 million due to misunderstanding and misinterpretation of period end cut-off procedures. Revenues were understated by approximately \$2.9 million, prior to audit adjustments, due to the inability to link business processes to accounting transactions and a lack of understanding of what transactions generate revenues.

Expenditures

Period end cut-off review, required by the Fiscal Year End Closing Instructions distributed by the Department of Finance & Management and necessary to ensure the completeness of accounts payable and expenditures, directed departments to review all vouchers and journals recorded in the first forty-five days after fiscal year end to determine whether associated goods or services were received or performed prior to period end.

During our testing of the period end cut-off process, we noted errors in approximately 19 percent of the items selected for testing (18 of 93 items). This high error rate indicates a systemic misunderstanding and/or misapplication of period end cut-off procedures.

Revenues

Limited guidance is provided to agencies regarding classification of revenues and the types of transactions which constitute revenue. The \$2.9 million understatement of revenue is net, derived from \$13.3 million in understatement errors and \$10.4 million of overstatement errors, as follows:

Appendix I

Schedule of Findings and Responses

- Agency financial personnel lacked understanding of a common revenue source for an agency and did not realize that a receivable related to this revenue source was under-reported by \$13.3 million as of June 30, 2006.
- Agency financial personnel lacked knowledge of a Generally Accepted Accounting Principles (“GAAP”) requirement to present receivables net of uncollectible amounts, therefore failing to consider the risk of uncollectibility in a significant new type of transaction and overstating revenue by approximately \$1.7 million.
- Agency financial personnel lacked understanding regarding the types of transactions that should be classified as revenues according to GAAP and overstated revenue by approximately \$8.7 million.

Recommendations

We recommend that the Secretary of the Agency of Administration implement two measures to address the need for technical accounting and financial expertise at the agencies.

- (1) Direct the Department of Finance & Management, in conjunction with the Department of Human Resources, to propose and oversee specific accounting and financial reporting training for business managers and accountants key to the financial reporting process.
- (2) Direct the Department of Finance & Management, in conjunction with the Department of Human Resources, to review the accounting and financial knowledge, skills and abilities listed in applicable job specifications for accounting and financial positions to determine whether the State is recruiting employees with sufficient and relevant experience.

Management’s Response and Planned Corrective Actions

In responding to a draft of this report, the Commissioner of the Department of Finance & Management stated that he agrees in part with this finding. He stated that the Department of Finance & Management does not have the responsibility for, nor is staffed to provide, workforce training. Nevertheless, the Commissioner outlined the training that is being provided, and is expected to be provided in the future, on the State’s financial system. In addition, the Commissioner stated that the Department has established quarterly business manager meetings (the first one of which was on January 10, 2007) that will be used to focus on knowledge sharing and training. The Commissioner also stated that his office will work with the Department of

Appendix I

Schedule of Findings and Responses

Human Resources to determine if functional accounting classes can or should be developed at the State's Cyprian Learning Center.

We agree that the duties of the Commissioner of the Department of Finance & Management outlined in 32 V.S.A §182 do not expressly require the Commissioner to conduct training. However, we believe that in order to fulfill the duties of the Commissioner contained in 32 V.S.A §182, (such as to "coordinate the fiscal procedures of the state including all departments, institutions and agencies"), it would behoove the Commissioner to take explicit actions, such as training, to ensure that agency/department personnel have the expertise to provide accurate accounting transactions. Nonetheless, we also believe that the Commissioner's plan to work with the Department of Human Resources on this issue is prudent. Accordingly, we modified our recommendation to reflect this relationship and to acknowledge that the Department of Finance & Management may not have to provide the training itself, but instead should be responsible for its oversight.

The Commissioner of the Department of Finance & Management also addressed our recommendation regarding the accounting and financial knowledge, skills and abilities listed in applicable job specifications for accounting and financial positions. He stated that the Agency of Administration had previously recognized that the State's financial staff did not always possess the requisite accounting skills. Accordingly, the Department of Human Resources has undertaken a review of all financial positions and had formed a job classification review committee that includes staff from other organizations, including the Department of Finance & Management. To recognize the key roles that the Departments of Finance & Management and Human Resources play in this process, we modified our recommendation to explicitly recognize that both organizations need to be involved in implementing this recommendation.

Control Finding #2006-3 Information Technology Controls

The data in the State's financial statements stem from a wide variety of systems managed by a myriad of internal and external organizations. It is critical that these organizations employ effective information technology (IT) controls so that State and citizen financial, programmatic, and other sensitive information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. Moreover, ineffective system controls can impair the accuracy, completeness, and timeliness of

Appendix I

Schedule of Findings and Responses

information used by management and increase the potential for undetected material misstatements in the State's financial statements.

As part of gaining an understanding of IT general controls² at five State environments³ we considered whether there were weaknesses in the design of their controls in the areas of (1) access to programs and data, (2) application and system software changes, and (3) computer operations. Our analysis determined that there were significant control weaknesses within each of the State environments. Confidential reports have been issued to each of the entities that were part of the assessment performed under the auspices of the financial statement audit that detail the weaknesses found as well as recommendations for improvement. The following provides a high-level summary of the results of the review.

- *Overall Security Planning.* Entities should have a written plan that clearly describes the entity's security program and policies and procedures that support it. The five entities reviewed did not have such plans.
- *Access to Data and Programs.* Access controls should provide reasonable assurance that computer resources are protected against unauthorized modification, disclosure, loss, or impairment. The entities' controls over access were mixed. For example, on the positive side, (1) the networks were configured to limit unauthorized access through the use of firewalls, (2) antivirus software had been installed on servers and personal computers and/or laptops, and (3) financial applications were configured to require a unique user ID and password identification. However, other critical controls, such as adequate password and access rights management were often deficient. Inadequate access controls diminish the reliability of computerized data and increase the risk of destructive or inappropriate disclosure of data.
- *Program Changes.* A disciplined process for testing and approving modified programs prior to their implementation is essential to make sure

²General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They create the environment in which application systems and controls operate.

³The five environments were those associated with the (1) Department of Information and Innovation's GOVNet wide-area-network and data center operations, (2) Department of Taxes' Vermont Integrated Revenue Collection System, Revenue and Receipt Accounting System, and Customer Information Control System, (3) Agency of Transportation's State Transportation Accounting and Reporting System, (4) Department of Labor's Vermont Automated Benefit System and Contribution Tax System, and (5) Agency of Human Services' ACCESS system.

Appendix I

Schedule of Findings and Responses

programs operate as intended and that no unauthorized changes are introduced. There were a wide variety of control exceptions in this area that largely stem from a lack of formal policies and procedures for approving, testing, and placing modifications into production. Another common weakness was controls over emergency changes. Without proper controls over software changes there is a risk that security features could be inadvertently or deliberately omitted or turned off or that processing irregularities or malicious code could be introduced.

- *Computer Operations.* Controls in this area address a wide variety of issues, such as controls over job processing, backup and recovery procedures, and problem management procedures. The five entities were generally strongest in implementing controls in computer operations. For example, no exceptions were found at any of the entities related to controls over backup media for systems and applications and the monitoring of the production environment to identify incidents and failures. However, weaknesses were found related to restoration testing of off-site data backup and disaster recovery plans. Without appropriate and periodic restoration tests, assurance cannot be placed on the reliability of backup media to recover key systems, applications, and data assets in the event of an emergency.

One factor that contributes to the IT general control weaknesses found in the five IT environments that were reviewed is that existing statewide security policies are outdated and are not comprehensive. This problem is not new. In 2002 we also reported that the State lacked critical security policies and protocols and made various recommendations related to the development of such documents.⁴ The Deputy Commissioner of the Department of Information and Innovation reported that the office has recently appointed a System Security Director and has formed an enterprise Security Policy Development Team, whose role is to identify and quantify risk, draft policy, and manage the policy development process. However, there is no explicit plan in place that details the tasks, resources, and milestones for the development of IT security policies and how compliance with the policies once developed will be achieved. According to the System Security Director, she is in the process of developing goals and a written plan for the security policy project that will be vetted and approved by the Security Policy Development Team.

⁴*Securing the Enterprise: A High-Level Assessment of Vermont's Information Technology Security and Data Recovery Policies*, February 19, 2002.

Appendix I

Schedule of Findings and Responses

Aside from the development of security policies, another concern is how enforcement of the new policies will be achieved. According to the Deputy Commissioner of the Department of Information and Innovation, regular security audits are to be part of the new policy process. However, the applicable IT statutes do not explicitly include IT security within the duties of the Commissioner of the Department of Information and Innovation.⁵ Accordingly, we question whether the Commissioner has sufficient authority to compel compliance with the security policies that are expected to be developed and the extent to which any security audits performed will be able to affect change. Explicit statutory authority that lays out the IT security responsibilities of the Commissioner and requires compliance with IT security policies can serve as a powerful enforcement mechanism as well as serve notice that IT security is considered vital to responsible governance and is a priority of the State.

Recommendations

We recommend that the Commissioner of the Department of Information and Innovation direct the Security Policy Development Team to develop a plan that details the tasks, resources, and milestones for the development of IT security policies and how compliance with the policies once developed will be achieved.

We recommend that the Legislature consider enacting legislation to bolster and support the role of the Commissioner of the Department of Information and Innovation for setting and enforcing IT security policies for Vermont State government as a whole.

Management's Response and Planned Corrective Actions

In response to this finding, the Commissioner of the Department of Finance & Management attached a memorandum that the Commissioner of the Department of Information and Innovation had previously provided to us in response to a confidential draft report that provided more specific information on our IT control findings related to this department. In this memorandum, the Commissioner of the Department of Information and Innovation reiterated that the Security Director has assembled a cross-agency policy team to draft updated security and privacy policies. However, the Commissioner did not address our recommendation that a plan be developed

⁵The Commissioner of the Department of Information and Innovation also serves as the State's Chief Information Officer.

Appendix I

Schedule of Findings and Responses

to guide this team. We continue to believe that such a plan is warranted and necessary to ensure that the cross-agency team has sufficient resources, stays on track, and is held accountable for meeting milestones.

The Commissioner of the Department of Information and Innovation also provided information related to other ongoing initiatives of his office. For example,

- A contractor has been retained to audit and test all interactive online/web applications to ensure that no security gaps exist.
- Agencies will be asked to inventory all systems, identify the type of data in the system, and apply a risk rating to the system.
- Mandatory employee awareness training is being developed.
- Beginning in fiscal year 2008, IT funding will not be authorized until all serious audit findings are addressed.

In addition, we continue to believe that the Legislature should consider enacting legislation to bolster and support the role of the Commissioner of the Department of Information and Innovation for setting and enforcing IT security policies.

Appendix II

Agency Comments



State of Vermont
Department of Finance & Management
109 State Street, Pavilion Building
Montpelier, VT 05620-0401
www.finance.state.vt.us

[phone] 802-828-2376
[fax] 802-828-2428

Agency of Administration

MEMORANDUM

TO: Thomas M. Salmon, State Auditor of Accounts
CC: Mike Smith, Sue Zeller, Brad Ferland, Nancy Collins, Tanya Morehouse, Tim Keefe
FROM: Jim Reardon, Commissioner
RE: Administration's Responses
DATE: February 16, 2007

Secretary Smith has asked me to respond to your letter dated February 7, 2007. We thank you for the opportunity to respond prior to the release of your report entitled *Fiscal Year 2006; Report on Internal Controls Over Financial Reporting and on Compliance with Laws and Regulations*. After reviewing the three control findings, our Agency responses are detailed below. Please let me know you require additional information or if I can be of further assistance.

Control Finding #2006-1 – Compilation of the Comprehensive Annual Financial Report

1. Inadequate Segregation of Duties:

- a. The Department of Finance & Management already has in place a knowledge transfer training program aimed at distributing key CAFR component preparation from the Director of State-wide Reporting to the state-wide reporting staff. We have made great strides in this area and will continue with our training efforts. For the FY 2006 CAFR preparation, we continued to expand on this goal by having the majority of fund compilations handled by staff and not the Director. Our goal for the FY2007 CAFR will be to expand on this shift of duties, with an ultimate goal of having the staff develop all statements and footnotes and the Director performing a review role only.
- b. The Department of Finance & Management has begun recruiting for a recently vacant senior level position reporting to the Director of State-wide Reporting. The ideal candidate will be one who is qualified to assume the bulk of the CAFR compilation, thereby freeing the Director to devote time to review and verification.
- c. Continuation of the knowledge transfer and filling the senior position will address both the segregation of duties issue as well as increasing the expertise within the division. Finance & Management will also investigate attendance by selected staff members to Government Finance Officers Association (GFOA) training seminars and certification programs.



Appendix II

Agency Comments

2. Limited monitoring of decentralized accounting process occurring at multiple agencies and departments.
 - a. Although staffing levels do not allow the Department of Finance & Management to directly monitor the quality and accuracy of the thousands of accounting transactions entered by agency and departmental staff in our decentralized environment, we do believe there are improvements to be made. Our relatively new division of Internal Controls has begun operational reviews of departments or specific processes, such as revenue recognition. Operational reviews are concluded by issuing a corrective action report to the audited agency/department and are supplemented by issuance of a related Best Practices document to the entire state-wide financial community.
 - b. Better training and the hiring of better qualified accounting staff in the agencies/departments is critical to the quality of the accounting transactions in a decentralized environment.

Control Finding #2006-2 – Technical Accounting and Financial Management Expertise

1. The Agency of Administration agrees in part with this finding. Finance & Management is not staffed nor do we have the responsibility for workforce training. There are 2 types of accounting training that is applicable to the state-wide accounting/financial staff: a) training for the more than 200 daily users of the VISION state-wide accounting system (400 more users registered – most are part-time or casual users); and 2) actual accounting and financial reporting training.
 - a. Finance & Management is currently in the process of training VISION users for the impending go-live of the VISION 8.8 upgrade. Training classes have begun in earnest as of last week in preparation of Go-Live. Once Go-Live is implemented and a period of post Go-Live support is ended, Finance & Management will return to their regularly scheduled VISION training program which was halted until implementation of the upgrade.
 - b. We continue to improve the VISION web-site which contains reference material for all VISION users: policies, procedures, forms, month-end and year-end procedures, and training material. The web-site also includes a section on Internal Control containing Best Practice documents for key financial processes and a quarterly newsletter to provide agencies and departments with articles on good business practices, internal controls, and responsibilities.
 - c. The creation of the Internal Controls division and the Change Management function has created an internal structure that enables Finance & Management to address a number of these training issues.
 - d. While we agree that a certain percentage of the Business Managers and state-wide accounting staff are sometimes lacking in true accounting knowledge, Finance & Management is not staffed for teaching accounting nor is workforce training one of our mandates. Prior to the implementation of VISION in 2001, true accounting expertise was not as critical a requirement as it is today. Hiring adequately educated/trained individuals into agency and departmental accounting and finance positions is the responsibility of agency and department heads and the Department

Appendix II

Agency Comments

of Human Resources. The Department of Human Resources has undertaken a review of all financial positions which will help in future hiring qualifications. (see finding 2006-2)

- e. We have established quarterly business manager meetings which will be used to focus on knowledge sharing and training encompassing many aspects of the business managers' role, including the importance and value of state-wide reporting and the annual audit. The first quarterly meeting was held on January 10, 2007.
 - f. Finance & Management will work with Human Resources to determine if functional accounting classes can or should be developed at the State's Cyprian Learning Center.
2. The Agency of Administration had previously recognized the fact that state-wide financial staff did not always possess the requisite accounting skills required to effectively record transactions in the VISION system as it relates to state-wide reporting. Therefore, in October 2006 the Department of Human Resources requested review materials (RFRs) for all financial/business/accounting positions in all agencies and departments, in order to do a comprehensive review of the classification for these jobs. This review is currently in process. The job classification review committee of six includes three senior accounting directors [Director of Financial Operations, Department of Finance & Management; Administrative Services Director, Agency of Natural Resources; Fiscal Operations Manager, Department for Children & Families] to provide expertise in accounting knowledge evaluation during the review process. This review is long overdue, and the primary reasons for the review are:
- a. The last comprehensive statewide review of these jobs was done in 1986.
 - b. We know that departments are having difficulty recruiting with the existing job series, job classes and the minimum qualifications associated with those jobs.
 - c. We need to update jobs, and job series to reflect the current fiscal and business world. We also want to reduce the number of unique job classes.
 - d. Of course, we want to ensure jobs are properly classified. However unlike some large reviews we are simply not sure how much pay grades will change, and are not certain that "upgrades" are necessary across the state.
 - e. The proper classification of financial jobs will result in the hiring of more qualified individuals with relevant work experience.

Control Finding #2006- 3 Information Technology Controls

Thomas Murray, Commissioner has previously provided a memo, dated 2/7/07 to State Auditor Salmon detailing his response. A Copy of Commissioner Murray's memo is attached for reference.

Appendix II

Agency Comments



Department of Information & Innovation Office of the Commissioner

MEMO TO: Thomas M. Salmon, CPA, State Auditor, Office of the Vermont State Auditor
FROM: Tom Murray, Commissioner and CIO, Department of Information & Innovation
CC: David Tucker, Deputy Commissioner, Department of Information & Innovation
DATE: February 7, 2007
RE: Official Comments on Findings and Recommendations Fiscal Year 2006 Audit

Thank you for providing the draft report "Computer Security: Results of Review at the Department of Information and Innovation. We appreciate the opportunity to work with your office on this important matter. We also appreciate the professionalism and collaborative effort of Linda Lambert from your staff and everyone at KPMG who worked on this audit.

As you know, we provided comments to the issues raised and they are included in Appendix I of this report. Rather than reiterate those comments here, I want to take the opportunity to update you on specific ones, including:

I.A.2. – Regarding the Security Plan comments, the Governor has directed DII to complete a comprehensive assessment of the state's vulnerabilities and to submit detailed action plan for addressing any concerns by March 1st. The following list outlines the activities that are underway and upcoming in this area.

Phase 1: Immediate Action Steps

1. **Policy:** DII Security Director has assembled a cross agency policy team to draft updated Security and Privacy Policies. The Data Protection Policy is complete, the Data Classification and Encryption Policy will be issued in February.
2. **Audits:** Bearhill Securities has been retained to audit and test all interactive online/web applications to ensure that no security gaps exist. Once this is completed the audit focus will shift to servers and applications.
3. **Inventory and Risk Assessment:** Agencies will be asked to inventory all systems, identify the type of data (confidential or public) and apply a risk rating to the system. All systems with confidential data will be required to submit a security plan and each system will be audited based on need and risk.

State of Vermont
133 State Street
Montpelier, VT 05633-0210

www.vermont.gov
phone: 802.828.4141
fax: 802.828.3398

Appendix II

Agency Comments

Memo to Thomas M. Salmon
February 7, 2007
Page 2

4. **DMZ Areas:** Over the coming months, all web applications and servers with internet user access will be required to move into one of two DMZ areas (Montpelier and Waterbury). These zones will have secure firewalls, and every measure will be taken to ensure the systems are maintained with the highest levels of Security.
5. **Encryption:** All laptops and portable devices with confidential data will be required to comply with encryption standards after March 1.
6. **Employee Training:** Mandatory employee awareness training is being developed and will be made available online in February and March for all state employees.

Phase 2: Long-term Action Steps

7. **Annual Audits:** Agency compliance audits will be required each year for servers and applications.
8. **Accountability:** Beginning in FY08 forward IT project funding will not be authorized until all serious audit findings are addressed.
9. **Web Consolidation:** The Web Portal Project is underway and will consolidate all state web sites into one secure environment with a redundant backup site.
10. **Server Consolidation:** The Server Consolidation Project is underway with the lease of new data center space at National Life and the completion of the data center on the Waterbury campus.
11. **Enterprise Focus:** The Enterprise Architecture Project is underway which will ensure all applications are developed and maintained with appropriate security throughout their life cycle.
12. **Statutory Authority:** A statute review is being completed with the Auditor's office to determine if additional language is needed to clarify the importance of security and the CIO's role.

I.B.7 – DII has met with the BGS staff responsible for operating the security system and has begun the process of restricting security access to the data center to only those individuals who really need it. We are also beginning a monthly review of the access list to ensure it is better managed in the future. We completed the requirement to create two zones for access to the data center, and are in the process of getting the lock changed on the back entrance and taking back any keys that were issued.

I.B.9 – We have hired an individual to manage the Technical Support Section and Data Center and will address this issue as soon as he is on board. He will be responsible for developing and implementing policies that are recommended in the report.

II.A.2 – DII has raised this issue with the mainframe user group that consists of the various departments and agencies that have processes running on the mainframe and notified them of the need to develop the policy. We understand that most of the mainframe users were also audited as part of this IT assessment and have similar findings in their reports.

Appendix II

Agency Comments

Memo to Thomas M. Salmon
February 7, 2007
Page 3

II.C.1 – See II.A.2 above.

II.E.1 – See II.A.2 above.

IV.C.1 – A contract has been executed and we are in the process of scheduling the independent review of the proposed mainframe processor upgrade.

Please let me know if I can provide additional information and comments.